UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/649,841	08/28/2000	Michael Charles Raley	111325-000002	7876

22204 7590 05/10/2005

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/649,841	RALEY, MICHAEL CHARLES	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/15/04, 12/09/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' amendment received on February 02, 2005.

2. Amendments to claims 1, 6-8 and 15 are acknowledged and that do not introduce any new matter.

3. Newly added claims 21-26 without introducing new matter is acknowledged.

4. Applicants' arguments have been fully considered but they are not persuasive.

5. Applicants on page 13 of the remarks argue that "While the '618 patent appears to disclose a client-server environment, there is no disclosure of a rights management module for receiving a request from the client for at least one of the documents and delivering the at least one document and a set of rights associated with the at least one document to the client as required by claim 1 of the present application. The Examiner points to the entire rights management section of the '618 patent to support his assertion that the '618 patent discloses a rights management module as previously recited in claim1 of the present application. But, upon examination, this section of the '618 patent merely discloses a way of managing electronic document rights. It does not, however, disclose the rights management module recited in claim 1 of the present application, as amended. To wit, the rights management module recited in claim 1, as

amended, is for receiving a request for at least one of the documents from the client and delivering the at least one document and a set of rights associated with and for enforcing use of the at least one document to the client by verifying the integrity of the client by confirming a user interface module is attached to the rendering engine, and by verifying the integrity of the rendering engine. As indicated beginning on page 13, line 4 of the present specification, the present invention includes a novel feature of using a standard, non-modified, rendering engine to leverage the existing infrastructure of content creation and distribution, while enabling the system of the invention with a new ability to limit the use of content that is distribute and made available in an unencrypted format to a rendering module."

Downs discloses a digital content distribution system having a right management scheme that its functions are implemented through a Clearinghouse (see col. 6, line 66-col. 7, line 18). Downs discloses that the Clearinghouse(s) are web sites accessible to the end-user(s) device(s) and in one embodiment the Clearinghouse(s) is part of the electronic digital content store(s) that provides (delivers) digital contents to consumers (i.e., end users) upon receiving a request(s) (see col. 9, lines 62-col. 10, line 3, col. 11, lines 24-28 and col. 81, lines 10-23). Downs also discloses that the usage conditions of a digital content (i.e., rights associated with a document) are included in the secure container (SC) and delivered to a user along with the content (see col. 6, lines 37-47, col. 9, lines 32-59 and col. 82, lines 15-22). Thus, Downs discloses that in one embodiment the rights management scheme, the Clearinghouse and the electronic digital content store are integrated in one entity that receives user(s) request(s) and

delivers digital content(s) to the user(s) to be used according to a set of usage conditions which meets the limitations of claim 1.

Downs further discloses that the Player Application (corresponding to the recited connection module) of the end-user device performs SC processing to enable rights management and processes watermark(s) of the digital content every time being used (col. 11, lines 35-52 and col. 81, lines 17-23). The performance of these functions indicates that the user interface is attached to the rendering engine and thus the integrity of the end-user device and the rendering engine are verified.

6. In light of the above submission the previous claim rejection under 35 USC § 102 is maintained while taken into account the new claims and the amendments to claims 1, 8 and 15 as follows.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-26 and are rejected under 35 U.S.C. 102(e) as being anticipated by Downs et al. (6,226,618 B1; hereinafter Down).

Downs discloses a digital content distribution system that securely provides encrypted data to a user (s) (col. 3, lines 40-55; col. 6, lines 35-54). An authorized user who has the right decryption key can decrypt the data. The encrypted data decryption key is sent first to a clearinghouse. At the clearinghouse the encrypted data decryption key is decrypted and re-encrypted using the user's public key and then transferred to the user's system.

Claim 1

Downs discloses:

a server having at least one document stored thereon in computer readable form (see, for example, col. 6, lines 35-54; col. 8, lines 55-67; Fig. 1D; col. 68, lines 40-45);

a client having a standard application program including a rendering engine capable of rendering unencrypted documents for viewing (see, for example, col. 11, lines 30-53; col. 33, lines 63-67; col. 79, lines 13-18, where the web browser corresponds to the recited a standard application program; col. 73, lines 12-20; col. 79, lines 47-50; Fig. 1D, item 198, where the helper application corresponds to the recited rendering engine);

a communications network coupled to said client and said server (see, for example, col. 6, lines 35-54);

a rights management module for receiving a request for at least one of the documents from said client and delivering the at least one document and a set of rights associated with and for enforcing use of the at least one document to said client (see, for example, col. 6, line 65-col. 7, line 55; col. 11, lines 30-53);

a connection module adapted to be attached to said rendering engine for receiving the list of rights associated with the at least one document, for verifying the integrity of the client by confirming a user interface module is attached to said rendering engine, and for verifying the integrity of the rendering engine (see, for example, col. 11, lines 30-53; Fig. 1D; col. 81, lines 17-23, where the Player Application of the end-user device corresponds to the recited a connection module connected to the helper application of the browser and performs secure container processing to enable rights management and processes watermark(s) of the digital content every time being used. The performance of these functions indicates that the user interface is attached to the rendering engine and thus the integrity of the end-user device and the rendering engine are verified);

a user interface module adapted to be attached to said rendering engine for controlling access by the client to the at least one document for enforcing use of the at least one document in accordance with the set of rights associated with said at least one document (see, for example, col. 6, lines 25-30; col. 7, lines 4-8; col. 7, lines 40-55; col. 47, lines 59-64; col. 81, lines 10-23).

Claim 2

Downs discloses:

A system as recited in claim 1, wherein said connection module is operative to detect whether said user interface module is attached to said rendering engine and for providing the at least one of the documents to said rendering engine if said user interface module is attached to said rendering

Drive (see, for example, col. 11, lines 30-53; Fig. 1D).

Claim 3

Downs discloses:

A system as recited in claim 2, wherein said connection module is operative to unencrypt the at least one of the documents (see, for example, Fig. 1D, item 195; Fig. 10, item 195; Fig. 15B, item 1505, where the Application Player decrypts the received information).

Claim 4

Downs discloses:

A system as recited in claim 2, wherein said standard application program is a Web browser and said server includes an HTTP server (see, for example, Fig. 1D, item 191; col. 68, lines 35-45).

Claim 5

Downs discloses:

A system as recited in claim 4, wherein said connection module and said user interface module attach to the rendering engine of the Web browser using at least one of ActiveX controls and plug-in technology (see, for example, Fig. 1D; Fig. 15B; col. 79, lines 26-40; col. 86, lines 10-18).

Claim 6

Downs discloses:

A system as recited in claim 4, wherein said rights management module comprises means for pointing to a start Web page stored on said server, and means for encrypting said means for pointing and wherein said connection module comprises means for unencrypting said means for pointing and wherein said system further comprises means for generating a secure start Web page which references said connection module and said means for pointing (see, for example, col. 7, lines 10-40).

Claim 7

Downs discloses:

A system as recited in claim 4, wherein said connection module comprises means for generating a signature and said rights management module comprises means for validating the signature, and wherein a request to said server is honored only if the signature is present and valid (see, for example, col. 13, lines 50-67; col. 14, lines 28-32; col. 14, lines 55-60; col. 16, lines 23-45; col. 19, lines 20-29; col. 28; lines 25-30).

Claim 8

Downs discloses:

A method for distributing and enforcing use of digital documents having one or more usage rights associated therewith, said method comprising the steps of (col. 3, lines 40-55; col. 6, lines 35-54):

storing at least one document on a server in computer readable form (see, for example, col. 6, lines 35-54; col. 8, lines 55-67; Fig. 1D; col. 68, lines 40-45);

accessing the server with a client having a standard application program including a rendering engine capable of rendering unencrypted documents (see, for example, col. 11, lines 30-53; col. 33, lines 63-67; col. 79, lines 13-18, where the Internet or the web browser corresponds to the recited a standard application program; col. 73, lines 12-20; col. 79, lines 47-50; Fig. 1D, item 198, where the helper application corresponds to the recited rendering engine);

receiving a request for at least one of the documents from the client (see, for example, col. 6, line 65-col. 7, line55; col. 11, lines 30-53);

delivering the at least one of the documents and a set of rights associated with and for enforcing use of the at least one of the documents to the client (see, for example, col. 6, line 65-col. 7, line55; col. 11, lines 30-53);

receiving the list of rights associated with the at least one of the documents with a connection module attached to the rendering engine and that verifyies the integrity of the client by confirming a user interface module is attached to said rendering engine, and for verifying the integrity of the rendering engine (see, for example, col. 11, lines 30-

53; Fig. 1D; col. 81, lines 17-23, where the Player Application of the end-user device corresponds to the recited a connection module connected to the helper application of the browser and performs secure container processing to enable rights management and processes watermark(s) of the digital content every time being used. The performance of these functions indicates that the user interface is attached to the rendering engine and thus the integrity of the end-user device and the rendering engine are verified);

controlling access by the client to the at least one of the documents for enforcing use of the at least one document in accordance with the set of rights associated with the at least one of the documents through a user interface module attached to the rendering engine (see, for example, col. 6, lines 25-30; col. 7, lines 4-8; col. 7, lines 40-55; col. 47, lines 59-64; col. 81, lines 10-23).

Claim 9

Downs discloses:

A method as recited in claim 8, further comprising the step of unencrypting the at least one of the documents (see, for example, Fig. 1D, item 195; Fig. 10, item 195; Fig. 15B, item 1505, where the Application Player decrypts the received information).

Claim 10

Downs discloses:

A method as recited in claim 8, further comprising the steps of detecting whether the user interface module is attached to the rendering engine and providing the at least one document to the rendering engine if the user interface module is attached to the rendering drive (see, for example, col. 11, lines 30-53; Fig. 1D).

Claim 11

Downs discloses:

A method as recited in claim 10, wherein said step of detecting further comprises determining whether said rendering engine has been compromised (see, for example, col. 80, lines 25-50, where the installed tamper resistant application on the end-user device corresponds to the recited determining whether said rendering engine has been compromised).

Claim 12

Downs discloses:

A method as recited in claim 10, wherein said standard application program is a Web browser and said server includes HTTP server software (see, for example, Fig. 1D, item 191; col. 68, lines 35-45).

Claim 13

Downs discloses:

A method as recited in claim 12, further comprising the steps of providing a pointer on the server to a start Web page stored on the server, encrypting the pointer, generating a secure start Web page on the server which references the pointer, providing access to the secure start Web page through the Web browser, and unencrypting the pointer on the client to provide the Web browser access to the start Web page on the server (see, for example, col. 7, lines 10-40).

Claim 14

Downs discloses:

A method as recited in claim 12, further comprising the steps of generating a signature with the client, transmitting the signature to the server with a request to the server, validating the signature with the server, and honoring the request only if the signature is present and valid (see, for example, col. 13, lines 50-67; col. 14, lines 28-32; col. 14, lines 55-60; col. 16, lines 23-45; col. 19, lines 20-29; col. 28; lines 25-30).

Claim 15

Downs discloses:

In a computer architecture including a server having documents stored thereon, a start page for accessing the documents, and a client running an application program having a rendering engine, a method of distributing and enforcing use of documents comprising the steps of (see, for example, col. 3, lines 40-55; col. 6, lines 35-54; col. 8, lines 55-67; Fig. 1D, Fig. 15A, Box 1510; col. 68, lines 40-45, where the Box 1510 of Fig. 1A displays a start page):

installing a rights management module on the server (see, for example, col. 6, line 65-col. 7, line 55);

attaching a user interface module and a connection module to the rendering engine (see, for example, col. 11, lines 30-53; Fig. 1D; col. 79, lines 25-35; col. 83, lines 45-60, where the Player Application corresponds to the recited a connection module and connected to the helper application of the browser)

creating a secure start page on the server (see, for example, col. 26, lines 51-57; col. 75, lines 10-20);

placing the documents in directory (see, for example, col. 6, lines 45-49; col. 67, lines 60-62);

programming the rights management module to include a pointer to the directory (see, for example, col. 6, line 65-col. 7, line 55; col. 7, lines 10-40);

encrypting an address to the directory (see, for example, col. 6, lines 52-56; col. 7, lines 16-40)

modifying the secure interface display to reference the user interface module and the start page (see, for example, col. 33, lines 62-67, Fig. I5A, Box 1510; col. 68, lines 20-30; col. 73, lines 13-30, where the extracted metadata which is displayed corresponds to the recited start page);

verifying the integrity of the client with the connection module by confirming a user interface module is attached to said rendering engine; verifying the integrity of the rendering engine with the connection module (see, for example, col. 11, lines 30-53; Fig. 1D; col. 81, lines 17-23, where the Player Application of the end-user device

corresponds to the recited a connection module connected to the helper application of the browser and performs secure container processing to enable rights management and processes watermark(s) of the digital content every time being used. The performance of these functions indicates that the user interface is attached to the rendering engine and thus the integrity of the end-user device and the rendering engine are verified);

unencrypting the address to the directory with the connection module to permit access to the start page and the documents on the server (see, for example, col. 73, lines 13-30, where the extracted metadata which is displayed corresponds to the recited start page).

enforcing use of the documents with the user interface module in accordance with a set of rights associated with the documents (see, for example, col. 6, lines 25-30; col. 7, lines 4-8; col. 7, lines 40-55; col. 47, lines 59-64; col. 81, lines 10-23).

Claim 16

Downs discloses:

A method as recited in claim 15, wherein the server includes HTTP server software, wherein the application program is a Web browser, wherein the secure interface display is a secure start Web page and wherein the address to the directory is in the form of a URL (see, for example, Fig. 1D, item 191; col. 18, step 129; col. 26, lines 40-46; col. 68, lines 35-45).

Claim 17

Downs discloses:

A method as recited in claim 16, further comprising the steps of:

accessing the secure start Web page by issuing a URL to the start page (see, for example, col. 26, lines 40-46; col. 28, lines 35-39);

directing the user interface module to the start page through the reference to the start page in the secure start Web page (see, for example, Fig. 15A, Box 1510; col. 84, lines 4-20);

creating an instance of the rendering engine (see, for example, Fig. 16, where the screen 1601 is a created instance of the rendering engine);

loading the start page in the instance of the rendering engine to display the start page on the client (see, for example, Fig. 16, where the screen 1601 is the start page displayed on the end-user device);

directing the instance of the rendering engine, under control of the user interface module, to retrieve one or more of the documents from the server. (see, for example, Fig. 16, where the screens 1602 and 1603 are the information (i.e., documents) retrieved through the user interface control).

Claim 18

Downs discloses:

A method as recited in claim 16, wherein said step of directing the instance comprises the steps of intercepting commands from the Web browser with the user

interface module and redirecting the commands through the connection module on the server (see, for example, col. 86, lines 10-18; Fig. 15B, where the interaction of different applications such as web browser and user interface is depicted in order to access to the server that contains digital content library 196).

Claim 19

Downs discloses:

A method as recited in claim 16, wherein said step of redirecting comprises the steps of instructing the instance to utilize a secure asynchronous protocol through the connection module (see, for example, col. 13, lines 27-33; col. 86, lines 10-18; col. 79, lines 10-20; col. 81, lines 10-22).

Claim 20

Downs discloses:

A method as recited in claim 16, further comprising the steps of validating, with the connection module, that the user interface module is attached to the rendering engine and permitting the client to connect to the server only if the validation step is positive (see, for example, col. 13, lines 50-67; col. 14, lines 28-32; col. 14, lines 55-60; col. 16, lines 23-45; col. 19, lines 20-29; col. 28; lines 25-30).

Claim 21

Downs discloses:

A system as recited in claim 1, wherein the connection module verifies the integrity of the rendering engine by verifying that the rendering engine has not been tampered with or otherwise compromised in a way that allows access to the at least one document in a way that bypasses the user interface module (see, for example, col. 11, lines 30-53; col. 80, lines 32-51, where the tamper resistant software on the user computer prevents unauthorized users to access a document that corresponds to preventing the bypass of the user interface module).

Claim 22

Downs discloses:

A system as recited in claim 1, wherein the rendering engine does not have direct access to the at least one document because the rendering engine is wrapped by the user interface module to prevent the rendering engine from performing prohibited functions outside of a scope of the set of rights associated with and for enforcing the use of the at least one document (see, for example, col. 7, lines 4-8; col. 7, lines 40-55; col. 80, lines 30-45; col. 81, lines 10-23, where a digital content is become accessible by the web browser based on the usage conditions and after it is decrypted by the player application using of a proper encryption key that corresponds to the recited the rendering engine is wrapped by the user interface module).

Claim 23

Downs discloses:

A method as recited in claim 8, wherein the step of verifying the integrity of the rendering engine includes verifying that the rendering engine has not been tampered with or otherwise compromised in a way that allows access to the at least one document in a way that bypasses the user interface module (see, for example, col. 11, lines 30-53; col. 80, lines 32-51, where the tamper resistant software on the user computer prevents unauthorized users to access a document that corresponds to preventing the bypass of the user interface module).

Claim 24

Downs discloses:

A method as recited in claim 8, further comprising wrapping the rendering engine with the user interface module so that the rendering engine does not have direct access to the at least one document to prevent the rendering engine from performing prohibited functions outside of a scope of the set of rights associated with and for enforcing the use of the at least one document (see, for example, col. 7, lines 4-8; col. 7, lines 40-55; col. 80, lines 30-45; col. 81, lines 10-23, where a digital content is become accessible by the web browser based on the usage conditions and after it is decrypted by the player application using of a proper encryption key that corresponds to the recited the rendering engine is wrapped by the user interface module).

Claim 25

Downs discloses:

A method as recited in claim 15, wherein the step of verifying the integrity of the rendering engine includes verifying that the rendering engine has not been tapered with or otherwise compromised in a way that allows access to the documents in a way that bypasses the user interface module (see, for example, col. 11, lines 30-53; col. 80, lines 32-51, where the tamper resistant software on the user computer prevents unauthorized users to access a document that corresponds to preventing the bypass of the user interface module).

Claim 26

Downs discloses:

A method as recited in claim 15, further comprising wrapping the rendering engine with the user interface module so that the rendering engine does not have direct access to the documents to prevent the rendering engine from performing prohibited functions outside of a scope of the set of rights associated with and for enforcing the documents (see, for example, col. 7, lines 4-8; col. 7, lines 40-55; col. 80, lines 30-45; col. 81, lines 10-23, where a digital content is become accessible by the web browser based on the usage conditions and after it is decrypted by the player application using of a proper encryption key that corresponds to the recited the rendering engine is wrapped by the user interface module).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN A.N.

May 6, 2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100